

## §§ 162.10–162.20

sending a renewal notice to the consumer before the expiration of the opt-out period, even if the consumer does not renew the opt-out election.

### §§ 162.10–162.20 [Reserved]

## Subpart B—Disposal Rules

### § 162.21 Proper disposal of consumer information.

(a) *In general.* Any covered affiliate must adopt must adopt reasonable, written policies and procedures that address administrative, technical, and physical safeguards for the protection of consumer information. These written policies and procedures must be reasonably designed to:

(1) Insure the security and confidentiality of consumer information;

(2) Protect against any anticipated threats or hazards to the security or integrity of consumer information; and

(3) Protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

(b) *Standard.* Any covered affiliate under this part who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(c) *Examples.* The following examples are “reasonable” disposal measures for the purposes of this subpart—

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed;

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed; and

(3) After due diligence, entering into and monitoring compliance with a written contract with another party engaged in the business of record destruction to dispose of consumer infor-

## 17 CFR Ch. I (4–1–14 Edition)

mation in a manner that is consistent with this rule.

(d) *Relation to other laws.* Nothing in this section shall be construed:

(1) To require a person to maintain or destroy any record pertaining to a consumer that is imposed under Sec. 1.31 or any other provision of law; or

(2) To alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

## Subpart C—Identity Theft Red Flags

SOURCE: 78 FR 23660, Apr. 19, 2013, unless otherwise noted.

### § 162.30 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) *Scope of this subpart.* This section applies to financial institutions or creditors that are subject to administrative enforcement of the FCRA by the Commission pursuant to Sec. 621(b)(1) of the FCRA, 15 U.S.C. 1681s(b)(1).

(b) *Special definitions for this subpart.* For purposes of this section, and Appendix B to this part, the following definitions apply:

(1) Account means a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes an extension of credit, such as the purchase of property or services involving a deferred payment.

(2) The term *board of directors* includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated senior management employee.

(3) *Covered account* means:

(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a margin account; and

(ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) *Credit* has the same meaning in Sec. 603(r)(5) of the FCRA, 15 U.S.C. 1681a(r)(5).

(5) *Creditor* has the same meaning as in 15 U.S.C. 1681m(e)(4), and includes any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that regularly extends, renews, or continues credit; regularly arranges for the extension, renewal, or continuation of credit; or in acting as an assignee of an original creditor, participates in the decision to extend, renew, or continue credit.

(6) *Customer* means a person that has a covered account with a financial institution or creditor.

(7) *Financial institution* has the same meaning as in 15 U.S.C. 1681a(t) and includes any futures commission merchant, retail foreign exchange dealer, commodity trading advisor, commodity pool operator, introducing broker, swap dealer, or major swap participant that directly or indirectly holds a transaction account belonging to a consumer.

(8) *Identifying information* means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any—

(i) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(ii) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(iii) Unique electronic identification number, address, or routing code; or

(iv) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

(9) *Identity theft* means a fraud committed or attempted using the identifying information of another person without authority.

(10) *Red Flag* means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(11) *Service provider* means a person that provides a service directly to the financial institution or creditor.

(c) *Periodic identification of covered accounts.* Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor shall conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) *Establishment of an Identity Theft Prevention Program*—(1) Program requirement. Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Identity Theft Prevention Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(2) *Elements of the Identity Theft Prevention Program.* The Identity Theft Prevention Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those Red Flags into its Identity Theft Prevention Program;

(ii) Detect Red Flags that have been incorporated into the Identity Theft

## § 162.31

## 17 CFR Ch. I (4–1–14 Edition)

Prevention Program of the financial institution or creditor;

(iii) Respond appropriately to any Red Flags that are detected pursuant to paragraph (d)(2)(ii) of this section to prevent and mitigate identity theft; and

(iv) Ensure the Identity Theft Prevention Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.

(e) *Administration of the Identity Theft Prevention Program.* Each financial institution or creditor that is required to implement an Identity Theft Prevention Program must provide for the continued administration of the Identity Theft Prevention Program and must:

(1) Obtain approval of the initial written Identity Theft Prevention Program from either its board of directors or an appropriate committee of the board of directors;

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Identity Theft Prevention Program;

(3) Train staff, as necessary, to effectively implement the Identity Theft Prevention Program; and

(4) Exercise appropriate and effective oversight of service provider arrangements.

(f) *Guidelines.* Each financial institution or creditor that is required to implement an Identity Theft Prevention Program must consider the guidelines in appendix B of this part and include in its Identity Theft Prevention Program those guidelines that are appropriate.

## § 162.31 [Reserved]

## § 162.32 Duties of card issuers regarding changes of address.

(a) *Scope.* This section applies to a person described in § 162.30(a) that issues a debit or credit card (card issuer).

(b) *Definition of cardholder.* For purposes of this section, a cardholder

means a consumer who has been issued a credit or debit card.

(c) *Address validation requirements.* A card issuer must establish and implement reasonable policies and procedures to assess the validity of a change of address if it receives notification of a change of address for a consumer's debit or credit card account and, within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account. Under these circumstances, the card issuer may not issue an additional or replacement card, until, in accordance with its reasonable policies and procedures and for the purpose of assessing the validity of the change of address, the card issuer:

(1)(i) Notifies the cardholder of the request:

(A) At the cardholder's former address; or

(B) By any other means of communication that the card issuer and the cardholder have previously agreed to use; and

(ii) Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

(2) Otherwise assesses the validity of the change of address in accordance with the policies and procedures the card issuer has established pursuant to § 162.30.

(d) *Alternative timing of address validation.* A card issuer may satisfy the requirements of paragraph (c) of this section if it validates an address pursuant to the methods in paragraph (c)(1) or (c)(2) of this section when it receives an address change notification, before it receives a request for an additional or replacement card.

(e) *Form of notice.* Any written or electronic notice that the card issuer provides under this paragraph must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.